Claim 35 (Previously Presented). The method of claim 31, wherein the predefined redirection criteria cause the problematic traffic to be redirected to a black hole.

Claim 36 (Previously Presented). The activity monitoring system of claim 26, wherein the route arbiter is coupled to a peering point located upstream from a plurality of edge devices.

Claim 37 (Previously Presented). The detection system of claim 1, wherein the activity monitoring system is incorporated into the switching device.

Claim 38 (Previously Presented). The detection system of claim 1, wherein the route arbiter is incorporated into the switching device and the traffic analyzer is maintained in a separate device.

Claim 39 (Previously Presented). The detection system of claim 1, wherein the traffic analyzer is incorporated into the switching device and the route arbiter is maintained in a separate device.

REMARKS

Claims 1 through 39 remain in this application. Claim 1 has been amended.

Claim Rejections-35 USC § 102(e)

In the Office Action, claims 1-13 and 16-39 are rejected under 35 USC 102(e) as being anticipated by Shanklin et al. (U.S. Patent No. 6, 578, 147.)

Claim 1

Claim 1 is being rejected as being unpatentable over Shanklin (6,578,147.) Claim 1 recites "a detection system for identifying and eliminating excessive requests for information on a network to prevent the failure of a portion of the network, comprising:

at least one switching device, wherein the switching device has predefined parameters for receipt of an acceptable volume of requests for information."

In order to anticipate an invention under 35 USC 102(e), the cited reference must contain all the limitations contained in a particular claim that the reference is deemed to anticipate. In the instant case, the present invention claims an intrusion detection system that identifies and eliminates excessive requests for information on a network and includes denial of service attacks. Thus, intrusion detections system whenever alluded to includes denial of service attacks. This intrusion detection is achieved by monitoring for abnormal traffic pattern, including but not limited to a high volume of request from a single IP address, numerous TCP-IP connect statements without any data requests or multiple attempts from an invalid address. (Specification Page 12, lines 26-28.) This limitation is not contained in the Shanklin reference, which merely discloses intrusion of detection by storing signatures of known intrusion from similar activities carried out earlier, comparing the incoming traffic to the stored signatures in real time and if a match is found, detecting an intrusion.

In the present invention, the claim is directed to a detection system that identifies and eliminates excessive request for information i.e in other words the system focuses on volume of traffic. This limitation is not present in Shanklin which merely discloses monitoring the content and context of the network traffic and matching it with stored signatures. As disclosed by Shanklin, if a match is found then intrusion is detected. (See Column 2, lines 65-67, Column 4, lines 62-67.)

Thus the present invention is not in any way anticipated by Shanklin. Accordingly, Applicants respectfully suggest that the § 102 (e) rejection to claim 1 be withdrawn and an indication of allowance be made.

Claims 2-7

In the Office Action claims 2-7 have also been rejected as being anticipated by Shanklin under 35 USC § 102(e). Claims 2-7 are dependent from Claim 1. As shown above, Shanklin does not disclose the limitations as disclosed in claim 1. Consequently, dependent claims 2-7 are not anticipated by Shanklin. In light of the above, Applicant respectfully requests that § 102(e) rejection to claims 2-7 be withdrawn and an indication of allowance be made.

Claim 8

In the Office Action claim 8 has been rejected as being anticipated by Shanklin under 35 USC § 102(e). In the instant case, the present invention claims a method for preventing the failure of a network device which has been configured to receive a predefined volume threshold of packets of information. In other words, the claim is directed to a method that identifies and eliminates excessive request for information by focusing on the volume of traffic. If the volume of traffic exceeds certain predefined threshold of acceptable volume, intrusion is detected. This limitation is not met by Shanklin which merely discloses intrusion detection by monitoring the content and context of the network traffic and matching it with stored signatures. (See Column 2, lines 65-67, Column 4, lines 62-67.) If a match is found then intrusion is detected. There is no monitoring of the volume and frequency of requests as is clearly claimed under claim 8.

Thus the present invention is not in any way anticipated by Shanklin. Accordingly, Applicants respectfully suggest that the § 102 (e) rejection to claim 8 be withdrawn and an indication of allowance be made.

Claims 9-10

In the Office Action claims 9-10 have also been rejected as being anticipated by Shanklin under 35 USC § 102(e). Claims 9-10 are dependent from Claim 8. As shown above, Shanklin does not disclose the limitations as disclosed in claim 8. Consequently, dependent claims 9-10 are not anticipated by Shanklin. In light of the above, Applicant respectfully requests that § 102(e) rejection to claims 9-10 be withdrawn and an indication of allowance be made.

Claim 11

In the Office Action, claim 11 has been rejected as being anticipated by Shanklin under 35 USC § 102(e). In the instant case, the present invention claims a process for identifying an intrusion and preventing the failure of a network device by monitoring the volume of traffic. This limitation is not met by Shanklin, which merely discloses comparing all incoming traffic to the stored signatures, which are in effect patterns that exist when the header information is changed to convey the impression that the network request is from a trusted source. (See Column 2, lines 65-67.)

The present invention also contains the limitation of "determining whether the first volume of traffic exceeds the predefined parameter of an acceptable volume of traffic from a transmitting source." In other words, the present limitation is directed to volume of traffic and determining if the volume exceeds a certain predefined threshold. This limitation is also not met by Shanklin which merely discloses intrusion detection through signature analysis by comparing the incoming traffic to the stored signatures. Signature analysis in Shanklin includes but is not limited to checksum verification, hop count checking, and option checking. (See Column 4, lines 33-38.) Shanklin merely discloses intrusion detection by monitoring the content and context of the network traffic and matching it with stored signatures. (See Column 2, lines 65-67, Column 4, lines 62-67.) If a match is found then intrusion is detected. There is no monitoring of the volume of requests as is clearly claimed under claim 11.

Further, the present invention contains the limitation of directing the traffic to the traffic analyzer once intrusion has been detected. Thus, the present invention prevents failure of a network device by directing the traffic away from the device to a traffic analyzer. On the other hand Shanklin does not contain this limitation. Shanklin merely discloses intrusion detection without disclosing a method to respond to such intrusion detection.

Thus the present invention as claimed in claim 11 is not in any way anticipated by Shanklin. Accordingly, Applicants respectfully suggest that the § 102 (e) rejection to claim 11 be withdrawn and an indication of allowance be made.

Claim 12

In the Office Action claim 12 has also been rejected as being anticipated by Shanklin under 35 USC § 102(e). Claim 12 is dependent from Claim 11. As shown above, Shanklin does not disclose the limitations as disclosed in claim 11. Consequently, dependent claim 12 is not anticipated by Shanklin. In light of the above, Applicant respectfully requests that § 102(e) rejection to claim 12 be withdrawn and an indication of allowance be made.

Claim 16

Claim 16 is being rejected as being unpatentable over Shanklin (6,578,147.) Claim 16 recites a system for identifying and eradicating fraudulent requests on a network, comprising an anomaly recognition module that "identifies fraudulent network requests in accordance with predefined anomaly criteria."

In order to anticipate an invention under 35 USC 102(e), the cited reference must contain all the limitations contained in a particular claim that the reference is deemed to anticipate. In the instant case, the present invention claims a system that identifies and eradicates fraudulent requests on a network. This is achieved by monitoring for abnormal traffic pattern, including but not limited to a high volume of request from a single IP address, numerous TCP-IP connect statements without any data requests or multiple attempts form an invalid address. (Specification Page 12, lines 26-29.) This limitation is not contained in the Shanklin reference, which merely discloses detection of intrusion by storing signatures of known intrusion from similar activities carried out earlier, comparing the incoming traffic to the stored signatures in real time and if a match is found, detecting an intrusion.

In the present invention, the claim is also directed to a system that identifies and eradicates excessive request for information i.e in other words the system focuses on volume of traffic. This limitation is not present in Shanklin which merely discloses monitoring the content and context of the network traffic and matches it with stored signatures. As disclosed by Shanklin, if a match is found then intrusion is detected.

Thus the present invention is not in any way anticipated by Shanklin. Accordingly, Applicants respectfully suggest that the § 102 (e) rejection to claim 16 be withdrawn and an indication of allowance be made.

Claim 17

Claim 17 is being rejected as being unpatentable over Shanklin (6,578,147.) Claim 17 recites a detection system, comprising "a switching device coupled to a network for providing access to network traffic, wherein the network traffic has predefined acceptable characteristics."

The present invention claims a detection system comprising a switching device that has been configured to receive a predefined volume threshold of packets of information. In other words, the claim is directed to a detection system that identifies excessive requests for information by monitoring the volume of traffic. This limitation is not met by Shanklin which merely discloses intrusion detection by monitoring the content and context of the network traffic and matching it with stored signatures. If a match is found then intrusion is detected. There is no monitoring of the volume of requests as is clearly claimed under claim 17.

Thus the present invention is not in any way anticipated by Shanklin. Accordingly, Applicants respectfully suggest that the § 102 (e) rejection to claim 17 be withdrawn and an indication of allowance be made.

Claim 19

Claim 19 is being rejected as being unpatentable over Shanklin (6,578,147.) Claim 19 recites an activity monitoring system comprising "a route arbiter coupled to a switching device, wherein the route arbiter monitors network activity on the switching device in accordance with predefined acceptable parameters."

In other words, the claim is directed to an activity monitoring system in which a route arbiter monitors network activity. If activity on the network exceeds predefined threshold, intrusion is detected. This limitation is not met by Shanklin which merely discloses intrusion detection by monitoring the content and context of the network traffic and matching it with stored signatures. If a match is found then intrusion is detected. There is not monitoring of the volume of requests as is clearly claimed under claim 19.

Further, the present invention in claim 19 claims a traffic analyzer that "redirects the network traffic in response to the route arbiter when the network activity exceeds the predefined acceptable parameters." Thus, the present invention claims directing the volume of traffic to the traffic analyzer if the volume exceeds the predefined volume parameter. This limitation is also not met by Shanklin, in which once intrusion is detected the attack is reported and logged and the misused connection is terminated. Thus, Shanklin does not disclose redirecting of traffic as claimed in the present invention.

Thus the present invention is not in any way anticipated by Shanklin. Accordingly, Applicants respectfully suggest that the § 102 (e) rejection to claim 19 be withdrawn and an indication of allowance be made.

Claim 20

In the Office Action claim 20 has also been rejected as being anticipated by Shanklin under 35 USC § 102(e). Claim 20 is dependent from Claim 19. As shown above, Shanklin does not disclose the limitations as disclosed in claim 19. Consequently, dependent claim 20 is not anticipated by Shanklin. In light of the above, Applicant respectfully requests that § 102(e) rejection to claim 20 be withdrawn and an indication of allowance be made.

Claim 21

Claim 21 is being rejected as being unpatentable over Shanklin (6,578,147.) Claim 21 recites a method for validating incoming packets from a network comprising "detecting a predefined condition associated with the incoming packets." In other words, the claim is directed to a method for identifying and eliminating excessive request for information i.e the system focuses on volume of traffic. This limitation is not met by Shanklin which merely discloses intrusion detection by monitoring the content and context of the network traffic and matching it with stored signatures. If a match is found then intrusion is detected. There is no monitoring of the volume of requests as is clearly claimed under claim 21.

Further, the present invention in claim 21 claims "instructing a switching device to direct the incoming packets to a traffic analyzer" if the volume exceeds the predefined volume parameter. On the other hand Shanklin does not contain this limitation. Shanklin merely discloses intrusion detection without disclosing a method to respond to such intrusion detection.

Thus the present invention is not in any way anticipated by Shanklin. Accordingly, Applicants respectfully suggest that the § 102 (e) rejection to claim 21 be withdrawn and an indication of allowance be made.

Claim 22

In the Office Action claim 22 has also been rejected as being anticipated by Shanklin under 35 USC § 102(e). Claim 22 is dependent from Claim 21. As shown above, Shanklin does not disclose the limitations as disclosed in claim 21. Consequently, dependent claim 21 is not anticipated by Shanklin. In light of the above, Applicant respectfully requests that § 102(e) rejection to claim 21 be withdrawn and an indication of allowance be made.

Claim 23

In the Office Action claim 23 has also been rejected as being anticipated by Shanklin under 35 USC § 102(e). Claim 23 is dependent from Claim 22. As shown above, Shanklin does not disclose the limitations as disclosed in claim 22. Consequently, dependent claim 23 is not anticipated by Shanklin. In light of the above, Applicant respectfully requests that § 102(e) rejection to claim 23 be withdrawn and an indication of allowance be made.

Claim 24

In the Office Action claim 24 has also been rejected as being anticipated by Shanklin under 35 USC § 102(e). Claim 24 is dependent from Claim 21. As shown above, Shanklin does not disclose the limitations as disclosed in claim 21. Consequently, dependent claim 24 is not anticipated by Shanklin. In light of the above, Applicant respectfully requests that § 102(e) rejection to claim 24 be withdrawn and an indication of allowance be made.

Claim 25

Claim 25 is being rejected as being unpatentable over Shanklin (6,578,147.) Claim 25 recites a system for preventing transmission of data on a network comprising "an activity monitoring module coupled to the router, wherein the activity monitoring module monitors the transmitted data in accordance with predetermined acceptance criteria and respond sin accordance with predetermined response criteria. In other words, the claim is directed to a system for preventing transmission of data on a network depending on abnormal traffic patterns such as excessive volume of requests. This limitation is not met by Shanklin which merely discloses intrusion detection by monitoring the content and context of the network traffic and matching it with stored signatures. If a match is found then intrusion is detected. There is no monitoring of the volume of requests as is clearly claimed under claim 25.

Claim 26

Claim 26 is being rejected as being unpatentable over Shanklin (6,578,147.) Claim 26 recites an activity monitoring system comprising a route arbiter that "monitors activity on the network in accordance with predefined acceptance criteria." In other words, this claim is directed to a system for monitoring nefarious activities on a network based on predefined criteria such as excessive volume of requests. This limitation is not met by Shanklin which merely discloses intrusion detection by monitoring the content and context of the network traffic and matching it with stored signatures. If a match is found then intrusion is detected. There is no monitoring of the volume of requests as is clearly claimed under claim 26.

Furthermore, the present invention in claim 26 claims an activity monitoring system in which abnormal traffic once detected is directed to the traffic analyzer. This limitation is also not met by Shanklin, in which once intrusion is detected the attack is reported and logged and the misused connection is terminated. Thus, Shanklin does not disclose redirecting of traffic as claimed in the present invention.

Thus the present invention is not in any way anticipated by Shanklin. Accordingly, Applicants respectfully suggest that the § 102 (e) rejection to claim 26 be withdrawn and an indication of allowance be made.

Claim 31

Claim 31 is being rejected as being unpatentable over Shanklin (6,578,147.) Claim 31 recites a method for preventing transmission of data on a network, comprising "identifying problematic data traffic on a network, in accordance with predefined traffic pattern criteria." In other words, this claim is directed to a system for monitoring nefarious activities on a network based on predefined criteria such as excessive volume of requests. This limitation is not met by Shanklin which merely discloses intrusion detection by monitoring the content and context of the network traffic and matching it with stored signatures. If a match is found then intrusion is detected. There is no monitoring of the volume of requests as is clearly claimed under claim 31.

Furthermore, the present invention in claim 31 claims "processing the problematic traffic in accordance with predefined redirection criteria." This limitation is also not met by Shanklin, in which once intrusion is detected the attack is reported and logged and the misused connection is terminated. (See Column 1, lines 35-38.) Thus, Shanklin does not disclose redirecting of traffic as claimed in the present invention.

Thus the present invention is not in any way anticipated by Shanklin. Accordingly, Applicants respectfully suggest that the § 102 (e) rejection to claim 31 be withdrawn and an indication of allowance be made.

Claim 32

In the Office Action claim 32 has also been rejected as being anticipated by Shanklin under 35 USC § 102(e). Claim 32 is dependent from Claim 31. As shown above, Shanklin does not disclose the limitations as disclosed in claim 31. Consequently, dependent claim 32 is not anticipated by Shanklin. In light of the above, Applicant respectfully requests that § 102(e) rejection to claim 32 be withdrawn and an indication of allowance be made.

Claim 33

In the Office Action claim 33 has also been rejected as being anticipated by Shanklin under 35 USC § 102(e). Claim 33 is dependent from Claim 31. As shown above, Shanklin does not disclose the limitations as disclosed in claim 31. Consequently, dependent claim 33 is not anticipated by Shanklin. In light of the above, Applicant respectfully requests that § 102(e) rejection to claim 33 be withdrawn and an indication of allowance be made.

Claim 34

In the Office Action claim 34 has also been rejected as being anticipated by Shanklin under 35 USC § 102(e). Claim 34 is dependent from Claim 31. As shown above, Shanklin does not disclose the limitations as disclosed in claim 31. Consequently, dependent claim 34 is not anticipated by Shanklin. In light of the above, Applicant respectfully requests that § 102(e) rejection to claim 34 be withdrawn and an indication of allowance be made.

Claim 35

In the Office Action claim 35 has also been rejected as being anticipated by Shanklin under 35 USC § 102(e). Claim 35 is dependent from Claim 31. As shown above, Shanklin does not disclose the limitations as disclosed in claim 31. Consequently, dependent claim 35 is not anticipated by Shanklin. In light of the above, Applicant respectfully requests that § 102(e) rejection to claim 35 be withdrawn and an indication of allowance be made.

Claim 36

In the Office Action claim 36 has also been rejected as being anticipated by Shanklin under 35 USC § 102(e). Claim 36 is dependent from Claim 26. As shown above, Shanklin does not disclose the limitations as disclosed in claim 26. Consequently, dependent claim 36 is not anticipated by Shanklin. In light of the above, Applicant respectfully requests that § 102(e) rejection to claim 36 be withdrawn and an indication of allowance be made.

Claim 37

In the Office Action claim 37 has also been rejected as being anticipated by Shanklin under 35 USC § 102(e). Claim 37 is dependent from Claim 1. As shown above, Shanklin does not disclose the limitations as disclosed in claim 1. Consequently, dependent claim 37 is not anticipated by Shanklin. In light of the above, Applicant respectfully requests that § 102(e) rejection to claim 37 be withdrawn and an indication of allowance be made.

Claim 38

In the Office Action claim 38 has also been rejected as being anticipated by Shanklin under 35 USC § 102(e). Claim 38 is dependent from Claim 1. As shown above, Shanklin does not disclose the limitations as disclosed in claim 1. Consequently, dependent claim 38 is not anticipated by Shanklin. In light of the above, Applicant respectfully requests that § 102(e) rejection to claim 38 be withdrawn and an indication of allowance be made.

Claim 39

In the Office Action claim 39 has also been rejected as being anticipated by Shanklin under 35 USC § 102(e). Claim 39 is dependent from Claim 1. As shown above, Shanklin does not disclose the limitations as disclosed in claim 1. Consequently, dependent claim 39 is not anticipated by Shanklin. In light of the above, Applicant respectfully requests that § 102(e) rejection to claim 39 be withdrawn and an indication of allowance be made.

Rejection under 35 USC 103

Claim 14

Claim 14 is being rejected as being unpatentable under 35 USC 103 over Potzulu (6,587, 432.) Claim 14 recites a method for detecting the best connection or path for transmitting traffic, where the volume of users determines the network load. This limitation is neither taught nor suggested by Potzulu because Potzulu merely discloses gathering information related to the congestion condition. Such information may include, the source and destination of such traffic, paths taken by the traffic, or other information which in turn may be used by the network administrator to cure the problem. (See Column 3, lines 35-43.) Potzulu does not teach or suggest detecting the best connection or path for transmitting traffic.

Thus the present invention is not in any way rendered obvious by Potzulu. Accordingly, Applicants respectfully suggest that the § 103 (a) rejection to claim 14 be withdrawn and an indication of allowance be made.

Claim 15

The Examiner also rejected claim 15 as being obvious over Potzulu in view of Beigi (US Patent No. 6,363,056) under 35 USC § 103(a). Claim 15 is dependent from Claim 14. As shown above, Potzulu does not teach or suggest the limitations as disclosed in claim 14. Consequently, dependent claim 15 is not rendered obvious under Potzulu. Further the Office Action admits that the limitation of analyzing the traffic load further comprising the step of transmitting a sample packet is not disclosed or even taught or suggested by Potzulu.

Beigi discloses computing round trip time for a probe packet but does not teach or suggest the limitation of analyzing the network load based on the volume of traffic as claimed in claim 15. Thus the present invention is not in any way rendered obvious by Potzulu in view of Beigi. In light of the above, Applicant respectfully requests that § 103(a) rejection to claim 15 be withdrawn and an indication of allowance be made.

CONCLUSION

In view of the foregoing, the Applicant believes that all of the claims are now in condition for allowance and respectfully request the Examiner to issue a timely Notice of Allowance in this case. If for any reason, the Examiner believes any of the claims are not in condition for allowance, he is encouraged to call the undersigned attorney at 650-325-4999 so that any remaining issues may be resolved.

The above changes are believed not to add new matter, as support is found is the specification as described above.

Claims 1-13 remain in this application. Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

Dennis S. Fernandez
Reg. No. 34,160

Date: 1/21/05

Address: **FERNANDEZ & ASSOCIATES LLP**
Patent Attorneys
1047 El Camino Real
Menlo Park, CA 94025

Customer No: **22877**

Phone: (650) 325-4999
Fax: (650) 325-1203
Email: *iploft@iploft.com*